CS 1511/2110 Midterm 2
Spring 2016

Directions

1. The test is closed book and closed notes.
2. There are 12 part B questions. Answer at most 9 part B questions. Please try to limit your answers to one sentence when possible. Part B questions are worth 10 points per question.
3. There are 5 part A questions. Answer at most 2 part A questions. Part A questions are worth 30 points per question.
4. Time will likely be an issue for most students. So use time wisely. Initially concentrate on the main ideas, and then fill in details with any remaining time.
5. In particular, for the part A questions, usually it is then a good idea for the start of your answer to define relevant terms, give an overview of the proof strategy/technique that you will use, and to explain the key ideas are. After this, you may launch into details.

PART B Questions

1. State the protocol for the interactive proof for graph non-isomorphism (GNI) given in the text and in class. You can assume that the verifier has access to private random bits that can not be seen by the prover.

2. State the perfect zero knowledge interactive proof for graph isomorphism.

3. Give a (formal as you can) definition of what it means for a private key protocol (presumably with small keys) to be semantically secure.

4. The Christian Science Monitor article you read as homework reported on the construction of a particular kind of quantum gate.

   (a) State the name of this type of gate.

   (b) Give the functionality (input /output relation) of this type of gate.

5. Give the matrix that represents the 2 bit Hadamard quantum operation.

6. (a) Define a $(f(n), g(n))$ restricted verifier, within the context of probabilistically checkable proofs.

   (b) Define $PCP(f(n), g(n))$.

   (c) State the PCP theorem.

7. Let S be the sum of two independent six sided dice. So the probability S is equal to x is $\frac{x-1}{36}$ for $2 \leq x \leq 7$, the probability S is equal to x is $\frac{13-x}{36}$ for $8 \leq x \leq 12$. Write an arithmetic expression for the entropy of S. You need not simplify this expression.

8. (a) Define the Komogorov complexity of a string x.

   (b) Let L be the language consisting of pairs (x, k) where x is a string, k is an integer, and the Kolmogorov complexity of x is equal to k. Is L in PSPACE? Justify your answer.

9. Explain how a pseudo-random generator can be used to derandomize a randomized algorithm to get a deterministic algorithm that is more efficient than the naive derandomization.

10. (a) Give the value of $u \times u$ when $u = 01$, where $\times$ is the outer/tensor product.

    (b) Give the Walsh-Hadamard encoding of $u \times u$ when $u = 01$.

11. Give a diagram to show which of the following statements imply other statements. So I'm looking for an organized list of implications, e.g. $(a) \Longrightarrow (c)$, $(c) \Longrightarrow (b)$, etc.

    (a) The existence of good pseudo-random generators

    (b) $P \neq NP$

    (c) The existence of computationally secure private key cryptography with small keys

    (d) The existence of secure public key cryptography

    (e) The existence of one-way functions

12. In the homework, you were assigned to read a blog article by Scott Aaronson on on Peter Shor's quantum algorithm for factoring.

    (a) According to this article, the problem of factoring was reduced to finding a particular property of a sequence. State this property.

    (b) To illustrate the intuition behind the algorithm, Professor Aaronson used a particular type of device that students frequently encounter in their day to day life. What is this device?

PART A Questions

1. Give a computationally zero knowledge interactive proof that a graph has a Hamiltonian cycle. Give a short informal explanation what "computationally zero knowledge" means, and intuitively why this proof this property.

2. Give the interactive proof (IP) protocol for showing that a particular Boolean formula F has a particular number k of satisfying assignments. Explain why the proof is correct.

3. The goal of this problem is to find a way to transmit information about a qubit by sending two classical bits. Alice and Bob split up entangled bits a and b in state $\frac{1}{\sqrt{2}}(|00> + |11>)$. Assume that now Alice is given qubit x. So x is in some unknown superposition between states $|0>$ and $|1>$. Alice now performs the following reversible CNOT operation on x: if a=1 then negate x. Alice then runs qubit a through a 1-bit Hadamard gate. Alice now measures the current values of a and x, and sends these two classical bits to Bob. Explain what the state of all the particles a, b, and x is after each of Alice's operations. Then explain how Bob can use the two classical particles to change the state of b to the original state of x.

4. Consider the proof that $NP \subseteq PCP(poly(n), 1)$ in the text and from class.

   (a) State the NP-complete problem for which a probabilistically checkable proof is given.

   (b) Explain what the format of the probabilistically checkable proof (the book).

   (c) Explain how the verifier determines whether the encoded solution is indeed a solution to the instance of the NP-complete problem, assuming that the encoding in the proof/book is in the correct format.

   (d) List the three properties the verifier has to check to make sure the encoding of the proof/book is of the correct form.

   (e) Pick one of these three properties, and explain how the verifier checks that the proof/book has this property.

5. Assume x is a letter that a sender wants to send to a receiver over a noisy channel, and let y be the letter received by the receiver. Because the channel is noisy, y may not equal x. For each pair (x, y) there is a probability that $P_{x,y}$ that the letter y is received when the letter x is sent. Let X be a probability distribution of the sent letter x, and Y the corresponding distribution of the received letter y. Let $I(X;Y)$ be the amount of information one gets about the sent letter x when one sees the received letter y. Let $I(Y;X)$ be the amount of information one gets about the received letter y when one sees the sent letter x. Is $I(X;Y) > I(Y;X)$, or is $I(Y;X) > I(X;Y)$ or is $I(X;Y) = I(Y,X)$? Justify/Prove that your answer is correct. Start with the standard definition of $I(X;Y)$.